Reception terminal, key management apparatus, and key updating method for public key cryptosystem

Publication number:	EP1249964 (A2)
Publication date:	2002-10-16
Inventor(s):	YOKOTA KAORU [JP]; TATEBAYASHI MAKOTO [JP]
Applicant(s):	MATSUSHITA ELECTRIC IND CO LTD [JP]
international:	H04L9/08; H04L9/30; H04L9/08; H04L9/28; (IPC1-7): G11B20/00; H04L9/08; H04L9/30
European:	
Application number:	EP20020008029 20020410
Priority number(s):	JP20010113667 20010412

Abstract of **EP 1249964 (A2)**

A method for use in a distribution system having a key management center, a distribution station and a reception terminal. The method updates a pair of distribution keys unique to the reception terminal, the distribution public key being used to encrypt distribution data, and the distribution secret key to decrypt encrypted data. In the key updating method, the reception terminal acquires an update secret key prior to data distribution, the keymanagement center acquires an update public key making a pair with update secret key, generates a new pair of distribution keys, encrypts new distribution secret key using update public key, transmits encrypted secret key to the reception terminal and updates to the new distribution public key. The reception terminal receives encrypted secret key and restores new distribution secret key by decrypting it using the update secret key and updates to the new distribution secret key.